IN THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF NORTH CAROLINA
WINSTON-SALEM DIVISION

TONI TURNAGE, individually and on behalf of all others similarly situated, Plaintiff, v. EMS MANAGEMENT AND CONSULTANTS, INC., Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY DEMAND**

Plaintiff Toni Turnage ("Plaintiff") brings this class action against Defendant EMS Management and Consultants, Inc. ("Defendant") for its failure to properly secure and safeguard Plaintiff's and Class Members' personally identifiable information ("PII") stored within Defendant's information network.

INTRODUCTION

1. Defendant is a billing services provider for emergency medical services.

2. Defendant acquired, collected, and stored Plaintiff's and Class Members' PII.

3. At all relevant times, Defendant knew or should have known, that Plaintiff and Class Members would use Defendant's services to store and/or share sensitive data, including highly confidential PII.

4. On no later than May 30, 2023, upon information and belief, unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PII as hosted with Defendant, with the intent of engaging in the misuse of the PII , including marketing and selling Plaintiff's and Class Members' PII.

5. The total number of individuals who have had their data exposed due to Defendant's failure to implement appropriate security safeguards is approximately 223,598.

6. Personally identifiable information ("PII") generally incorporates information that can be used to distinguish or trace an individual's identity, and is generally defined to include certain identifiers that do not on their face name an individual, but that is considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

7. The vulnerable and potentially exposed data at issue of Plaintiff and the Class stored on Defendant's information network, includes, without limitation: names, Social Security numbers, and dates of birth.

8. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII was safeguarded, failing to take available steps to prevent unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use.

9. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiff and Class Members in the future.

10. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are thus entitled to injunctive and other equitable relief.

I. JURISDICTION AND VENUE

11. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is over 100, many of whom reside outside the state of North Carolina

and have different citizenship from Defendant.[1] Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A)

12. This Court has jurisdiction over Defendant because Defendant operates in this District.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is located in this District, a substantial part of the events giving rise to this action occurred in this District, and Defendant has harmed Class Members residing in this District.

II. THE PARTIES

14. Plaintiff Toni Turnage is an adult individual and, at all relevant times herein, a resident and citizen of Albertson, North Carolina. Plaintiff received a letter from Defendant, dated August 9, 2023, stating that their PII was involved in the Data Breach (the "Notice").

15. Defendant EMS Management and Consultants, Inc., is a North Carolina corporation with its principal place of business located at 2540 Empire Drive, Ste. 100, Winston-Salem, NC 27103.

[1] According to the breach report submitted to the Office of the Maine Attorney General, 788 Maine residents were impacted in the Data Breach. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/d14bbac2-e6ce-40c2-8324-814e8b08a6ab.shtml (last accessed Sep. 26, 2023).

16. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Plaintiff.

17. Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of the responsible parties when their identities become known.

III. COMMON FACTUAL ALLEGATIONS

A. Defendant's Failed Response to the Breach

18. Not until after months it claims to have discovered the Data Breach did Defendant begin sending the Notice to persons whose PII Defendant confirmed was potentially compromised as a result of the Data Breach.

19. The Notice included, *inter alia*, basic details of the Data Breach, Defendant's recommended next steps, and Defendant's claims that it had learned of the Data Breach on July 12, 2023, and completed a review thereafter.

20. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PII with the intent of engaging in the misuse of the PII, including marketing and selling Plaintiff's and Class Members' PII.

21. The attack concerned MOVEit software, used by organizations (including Defendant) to securely send and receive sensitive data.[2] The vulnerability exploited by the hackers, who demanded ransom for the exfiltrated data, was something known as a "zero-day" vulnerability, meaning "a vulnerability in a system or device that has been disclosed but is not yet patched."[3]

22. Defendant had and continues to have obligations created by applicable federal and state law as set forth herein, reasonable industry standards, common law, and its own assurances and representations to keep Plaintiff's and Class Members' PII confidential and to protect such PII from unauthorized access.

23. Plaintiff and Class Members were required to provide their PII to Defendant in order to receive healthcare, and as part of providing healthcare, Defendant created, collected, and stored Plaintiff and Class Members with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

[2] https://www.jdsupra.com/legalnews/ems-management-and-consultants-inc-7680549/ (last accessed August 22, 2023).
[3] https://www.trendmicro.com/vinfo/us/security/definition/zero-day-vulnerability (last accessed August 17, 2023).

24. Despite this, Plaintiff and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used, and what steps are being taken, if any, to secure their PII going forward.

25. Plaintiff and Class Members are, thus, left to speculate as to where their PII ended up, who has used it, and for what potentially nefarious purposes, and are left to further speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities to prevent further breaches.

26. Unauthorized individuals can now easily access the PII and/or financial information of Plaintiff and Class Members.

B. Defendant Collected/Stored Class Members' PII

27. Defendant acquired, collected, and stored and assured reasonable security over Plaintiff's and Class Members' PII.

28. As a condition of its relationships with Plaintiff and Class Members, Defendant required that Plaintiff and Class Members entrust Defendant with highly sensitive and confidential PII.

29. Defendant, in turn, stored that information in the part of Defendant's system that was ultimately affected by the Data Breach.

30. By obtaining, collecting, and storing Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known

that they were thereafter responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

31. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

32. Plaintiff and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

33. Defendant could have prevented the Data Breach, which began no later than May 30, 2023, by adequately securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiff's and Class Members' PII.

34. Defendant's negligence in safeguarding Plaintiff's and Class Members' PII is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

35. Yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and Class Members' PII from being compromised.

C. Defendant Had an Obligation to Protect the Stolen Information

36. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce."[4]

37. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

38. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Plaintiff and Class Members.

39. Defendant owed a duty to Plaintiff and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that the PII was adequately secured and protected.

[4] The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

40. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

41. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach in its data security systems in a timely manner.

42. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

43. Defendant owed a duty to Plaintiff and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust this PII to Defendant.

44. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

45. Defendant owed a duty to Plaintiff and Class Members to encrypt and/or more reliably encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

D. Value of the Personally Identifiable Information

46. PII are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

47. Numerous sources cite dark web pricing for stolen identity credentials; for example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200[5]; Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web[6]; and other sources report that criminals can also purchase access to entire company data breaches from $999 to $4,995.[7]

48. Identity thieves can use PII , such as that of Plaintiff and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims—for instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or

[5] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed August 22, 2023).
[6] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed August 22, 2023).
[7] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed August 22, 2023).

identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

49. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used: according to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data might be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[8]

50. Here, Defendant knew of the importance of safeguarding PII and of the foreseeable consequences that would occur if Plaintiff's and Class Members' PII were stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of a breach of this magnitude.

51. As detailed above, Defendant is a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its

[8] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed August 22, 2023).

statutory and common law duties to Plaintiff and Class Members. Therefore, its failure to do so is intentional, willful, reckless and/or grossly negligent.

52. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PII and/or financial information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

E. Plaintiff's Experience

53. Plaintiff was a client of Defendant's, and their information was stored with Defendant as a result of their dealings with Defendant.

54. As required in order to obtain services from Defendant, Plaintiff provided Defendant with highly sensitive personal who then possessed and controlled it.

55. As a result, Plaintiff's information was among the data accessed by an unauthorized third-party in the Data Breach.

56. At all times herein relevant, Plaintiff is and was a member of the Class.

57. Plaintiff received a letter from Defendant, dated August 9, 2023, stating that their PII was involved in the Data Breach (the "Notice").

58. Plaintiff was unaware of the Data Breach—or even that Defendant had possession of their data until receiving that letter.

59. As a result, Plaintiff was injured in the form of lost time dealing with the consequences of the Data Breach, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring their accounts with heightened scrutiny and time spent seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach.

60. Plaintiff was also injured by the material risk to future harm they suffer based on Defendant's breach; this risk is imminent and substantial because Plaintiff's data has been exposed in the breach, the data involved, including her Social Security number, is highly sensitive and presents a high risk of identity theft or fraud; and it is likely, given Defendant's clientele, that some of the Class's information that has been exposed has already been misused.

61. Plaintiff suffered actual injury in the form of damages to and diminution in the value of their PII—a condition of intangible property that they entrusted to Defendant, which was compromised in and as a result of the Data Breach.

62. Plaintiff, as a result of the Data Breach, has increased anxiety for their loss of privacy and anxiety over the impact of cybercriminals accessing, using, and selling their PII and/or financial information.

63. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII, in combination with their name, being placed in the hands of unauthorized third parties/criminals.

64. Plaintiff has a continuing interest in ensuring that their PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

IV. CLASS ACTION ALLEGATIONS

65. Plaintiff brings this nationwide class action on behalf of themself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

66. The Class that Plaintiff seeks to represent is defined as follows:

> **Nationwide Class:**
>
> All individuals within the United States of America whose PII and/or financial information was exposed to unauthorized third-parties as a result of the data breach experienced by Defendant on May 30, 2023 (the "Class").

67. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

68. Plaintiff reserves the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

69. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. At least 223,000 individuals were notified by Defendant of the Data Breach, according to the breach report submitted to Office of the Maine Attorney General.[9] The Class is apparently

[9] https://apps.web.maine.gov/online/aeviewer/ME/40/d14bbac2-e6ce-40c2-8324-814e8b08a6ab.shtml (last visited Sep. 26, 2023).

identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

70. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

71. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

72. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as

a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

73. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that they has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

74. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who

could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

75. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

76. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

77. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

78. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

79. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

80. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiff and the class of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

V. CLAIMS FOR RELIEF

COUNT ONE
Negligence
(On behalf of Plaintiff and the Class)

81. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

82. At all times herein relevant, Defendant owed Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the PII of Plaintiff and Class Members in its computer systems and on its networks.

83. Among these duties, Defendant was expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession;

b. to protect Plaintiff's and Class Members' PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to detect the Data Breach quickly and to timely act on warnings about data breaches; and

d. to promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

84. Defendant knew that the PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

85. Defendant knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security.

86. Defendant knew about numerous, well-publicized data breaches.

87. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class Members' PII.

88. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PII that Plaintiff and Class Members had entrusted to it.

89. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their PII.

90. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Plaintiff and Class Members, Defendant had a duty to adequately protect its data systems and the PII contained therein.

91. Plaintiff's and Class Members' willingness to entrust Defendant with their PII was predicated on the understanding that Defendant would take adequate security precautions.

92. Moreover, only Defendant had the ability to protect its systems and the PII is stored on them from attack. Thus, Defendant had a special relationship with Plaintiff and Class Members.

93. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class Members' PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant, Plaintiff, and/or the remaining Class Members.

94. Defendant breached its general duty of care to Plaintiff and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiff and Class Members;

b. by failing to timely and accurately disclose that Plaintiff's and Class Members' PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII;

d. by failing to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiff and Class Members, misuse the PII and intentionally disclose it to others without consent.

e. by failing to adequately train its employees not to store PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class Members' PII;

g. by failing to implement processes to detect data breaches, security incidents, or intrusions quickly; and

h. by failing to encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

95. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

96. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages.

97. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII to Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PII.

98. Defendant breached its duty to notify Plaintiff and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Plaintiff and Class Members and then by failing and continuing to fail to provide Plaintiff and Class Members sufficient information regarding the breach.

99. To date, Defendant has not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and Class Members.

100. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII.

101. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members.

102. Plaintiff's and Class Members' PII was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

103. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

104. The damages Plaintiff and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

105. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery

from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft; (vi) lost continuity in relation to their healthcare; (vii) the continued risk to their PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

106. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

107. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to

undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT TWO
Breach of Implied Contract
(On behalf of Plaintiff and the Class)

108. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

109. Through its course of conduct, Defendant, Plaintiff and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII.

110. Defendant required Plaintiff and Class Members to provide and entrust their PII as a condition of obtaining Defendant's services.

111. Defendant solicited and invited Plaintiff and Class Members to provide their PII as part of Defendant's regular business practices.

112. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

113. As a condition of being clients of Defendant, Plaintiff and Class Members provided and entrusted their PII to Defendant.

114. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such

non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

115. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII to Defendant, in exchange for, amongst other things, the protection of their PII.

116. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

117. Defendant breached its implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

118. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

COUNT THREE
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of Plaintiff and the Class)

119. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

120. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

121. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendant.

122. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PII and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

123. Defendant acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT FOUR
Unjust Enrichment
(On behalf of Plaintiff and the Class)

124. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

125. By its wrongful acts and omissions described herein, Defendant has obtained a benefit by unduly taking advantage of Plaintiff and Class Members.

126. Defendant, prior to and at the time Plaintiff and Class Members entrusted their PII to Defendant for the purpose of obtaining health services, caused Plaintiff and Class Members to reasonably believe that Defendant would keep such PII secure.

127. Defendant was aware, or should have been aware, that reasonable patients and consumers would have wanted their PII kept secure and would not have contracted with Defendant, directly or indirectly, had they known that Defendant's information systems were sub-standard for that purpose.

128. Defendant was also aware that, if the substandard condition of and vulnerabilities in its information systems were disclosed, it would negatively affect Plaintiff's and Class Members' decisions to seek services therefrom.

129. Defendant failed to disclose facts pertaining to its substandard information systems, defects, and vulnerabilities therein before Plaintiff and Class

Members made their decisions to make purchases, engage in commerce therewith, and seek services or information.

130. Instead, Defendant suppressed and concealed such information. By concealing and suppressing that information, Defendant denied Plaintiff and Class Members the ability to make a rational and informed purchasing and health care decision and took undue advantage of Plaintiff and Class Members.

131. Defendant was unjustly enriched at the expense of Plaintiff and Class Members, as Defendant received profits, benefits, and compensation, in part, at the expense of Plaintiff and Class Members; however, Plaintiff and Class Members did not receive the benefit of their bargain because they paid for products and/or health care services that did not satisfy the purposes for which they bought/sought them.

132. Since Defendant's profits, benefits, and other compensation were obtained improperly, Defendant is not legally or equitably entitled to retain any of the benefits, compensation or profits it realized from these transactions.

133. Plaintiff and Class Members seek an Order of this Court requiring Defendant to refund, disgorge, and pay as restitution any profits, benefits and other compensation obtained by Defendant from its wrongful conduct and/or the establishment of a constructive trust from which Plaintiff and Class Members may seek restitution.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themself and each member of the Class, respectfully requests that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify the Proposed Class under N.C. G.S. § 1A-1, Rule 23 including the appointment of Plaintiff's counsel as Class Counsel;
2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;
3. That the Court enjoin Defendant, ordering them to cease from unlawful activities;
4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;
5. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of

Plaintiff and Class Members, including but not limited to an Order:

a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

c. requiring Defendant to delete and purge the PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems periodically;

f. prohibiting Defendant from maintaining Plaintiff's and Class Members' PII on a cloud-based database;

g. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

h. requiring Defendant to conduct regular database scanning and securing checks;

i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

k. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to monitor Defendant's networks for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested, and updated; and

l. requiring Defendant to meaningfully educate all Class Members about the threats they face due to the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorney's fees, costs, and litigation expenses, as allowed by law; and

8. For all other Orders, findings, and determinations identified and sought in this Complaint.

VII. JURY DEMAND

Plaintiff, individually and on behalf of the Class, hereby demands a trial by jury for all issues triable by jury.

Dated: September 27, 2023 Respectfully submitted,

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC

/s/ Scott C. Harris
Scott C. Harris (SBN 35328)
900 W. Morgan Street
Raleigh, North Carolina 27603
Phone: (919) 600-5000
sharris@milberg.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
5335 Wisconsin Avenue NW
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

LAUKAITIS LAW LLC
Kevin Laukaitis*
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

**Pro Hac Vice admission forthcoming*

Attorneys for Plaintiff and the Proposed Class